CLAIMS

1	1.	A method of providing anonymous digital cash, said method comprising:	
2		providing an entity with a secure co-processor;	
3		a user establishing a secure channel to a program running on said coprocessor;	
4	and		
5		the user sending a coin to be digitally signed to the coprocessor using any	
6	secur	e digital signature algorithm.	
1	2.	A method according to Claim 1, further comprising the steps of:	
2		the processor providing a signature to authenticate;	
3		the user using said coin for payment to a merchant; and	
4		the merchant returning the signed coin to the entity for credit to an account of	
5	the merchant.		
1 2	3.	A method of creating and managing electronic cash, comprising the steps:	
3	a customer communicating to a secure cryptography generator an encryption scheme		
4	and a cash amount;		
5	establishing a unit representing the cash amount;		
6	signing the unit;		
7	using the secure cryptography generator to encrypt the signed unit using the		
8	encryption scheme;		
9	storing in a database the encrypted signed unit and a value for the unit;		
10	transmitting the encrypted signed unit to the customer;		
11	the c	the customer decrypting the encrypted signed unit to obtain the signed unit; and	
12	neine	using the signed unit as a navment	

- 1 4. A method according to Claim 3, further including the steps of:
- 2 establishing an expiration date for the unit; and
- 3 storing the expiration date in the database.
- 1 5 A method according to Claim 3, wherein the signing step includes the step of
- 2 using the secure cryptography generator to sign the unit.
- 1 6. A method according to Claim 3, wherein the signing step includes the step of
- 2 signing the unit with a non-homomorphic signature.
- 1 7. A system for creating and managing electronic cash, comprising the steps:

2

- 3 a secure cryptography generator, including means for receiving an encryption scheme
- 4 and a cash amount from a customer;
- 5 means for establishing a unit representing the cash amount;
- 6 means for signing the unit;
- 7 wherein the secure cryptography generator encrypt the signed unit using the
- 8 encryption scheme;
- 9 a database for storing the encrypted signed unit and a value for the unit;
- 10 means for transmitting the encrypted signed unit to the customer; and
- means for the customer to decrypt the encrypted signed unit to obtain the signed unit,
- wherein the customer is able to use the signed unit as a payment.
- 1 8. A system according to Claim 7, further including means for establishing an
- 2 expiration date for the unit, and wherein
- 3 the expiration date is stored in the database.
- 1 9. A system according to Claim 7, wherein the secure cryptography generator
- 2 includes means for signing the unit.

- 1 10. A system according to Claim 7, wherein the means for signing includes means
- 2 for signing the unit with a non-homomorphic signature.
- 1 11. A program storage device readable by machine, tangibly embodying a program
- 2 of instructions executable by the machine to perform method steps for creating and
- 3 managing electronic cash, said method steps comprising:

4

- 5 using a secure cryptography generator to receive from a customer an encryption
- 6 scheme and a cash amount;
- 7 establishing a unit representing the cash amount;
- 8 signing the unit;
- 9 using the secure cryptography generator to encrypt the signed unit using the
- 10 encryption scheme;
- storing in a database the encrypted signed unit and a value for the unit;
- transmitting the encrypted signed unit to the customer;
- decrypting the encrypted signed unit to obtain the signed unit; and
- 14 using the signed unit as a payment.
- 1 12. A program storage device according to Claim 11, wherein said method steps
- 2 further include the steps of:
- 3 establishing an expiration date for the unit; and
- 4 storing the expiration date in the database.
- 1 13. A program storage device according to Claim 11, wherein the signing step
- 2 includes the step of using the secure cryptography generator to sign the unit.
- 1 14. A program storage device according to Claim 13, wherein the signing step
- 2 includes the step of signing the unit with a non-homomorphic signature.